Muster-Prüfprogramm

Privilegierte Zugriffe

12 Prüfschritte · NIS2, ISO 27001, BSI

12 Prüfschritte mit Kriterium, Fundstelle, Prüfhandlung und erwarteten Nachweisen. 8 Unterlagen zur Anforderung und die typischen Feststellungen.

NIS2-Richtlinie Art. 21 Abs. 2 lit. i · ISO/IEC 27001:2022 Anhang A 8.2 · BSI ORP.4 · ISO/IEC 27001:2022 Anhang A 8.2 und 5.15 · NIS2-Richtlinie Art. 21 Abs. 2 lit. j · § 30 Abs. 2 Nr. 10 BSIG · ISO/IEC 27001:2022 Anhang A 8.15 und 8.2 · ISO/IEC 27001:2022 Anhang A 5.18 und 8.2 · ISO/IEC 27001:2022 Anhang A 5.19 und 8.2 · ISO/IEC 27001:2022 Anhang A 5.18

Prüfungsziel und Geltungsbereich

Die Prüfung beurteilt, ob die Organisation privilegierte Zugriffe gezielt steuert: Inventar und Verantwortlichkeit, Beschränkung auf das Notwendige, zusätzliche Authentifizierung, geschützte Aufbewahrung der Zugangsdaten, Protokollierung der Nutzung und regelmäßige Überprüfung. Sie beurteilt außerdem, ob Notfallzugriffe und Zugriffe von Dienstleistern geregelt sind.

GELTUNGSBEREICH

- Administratorkonten für Betriebssysteme, Datenbanken, Verzeichnisdienste, Netzkomponenten, Virtualisierung und Cloud-Konsolen
- Technische Konten, Dienstkonten und Notfallkonten mit erhöhten Rechten
- Zugriffe von Dienstleistern mit privilegierten Rechten
- Nicht Gegenstand: das allgemeine Berechtigungsmanagement für normale Benutzer, das in einem eigenen Muster behandelt wird

Prüfschritte 1 bis 3

Schritt 01 NIS2-Richtlinie Art. 21 Abs. 2 lit. i; ISO/IEC 27001:2022 Anhang A 8.2

Eine Richtlinie regelt Vergabe, Nutzung und Entzug privilegierter Rechte und ist von der Leitung freigegeben.

Prüfhandlung Richtlinie lesen, Freigabe und Aktualität feststellen und den Geltungsbereich mit der Systemübersicht abgleichen.

Nachweise Richtlinie mit Freigabevermerk, Systemübersicht

Schritt 02 ISO/IEC 27001:2022 Anhang A 8.2; BSI ORP.4

Alle privilegierten Konten sind inventarisiert, jedem Konto sind eine verantwortliche Person und ein Zweck zugeordnet.

Prüfhandlung Privilegierte Konten direkt aus fünf Systemen auslesen und mit dem Inventar abgleichen.

Nachweise Inventar privilegierter Konten, Systemauszüge der Administratorgruppen

Schritt 03 ISO/IEC 27001:2022 Anhang A 8.2 und 5.15

Privilegierte Rechte sind auf das Notwendige beschränkt, Rollen sind fachlich begründet und genehmigt.

Prüfhandlung Zehn privilegierte Konten auswählen und Begründung sowie Genehmigung der Rechte prüfen.

Nachweise Anträge und Genehmigungen, Rollenbeschreibungen

Prüfschritte 4 bis 6

Schritt 04 — BSI ORP.4; ISO/IEC 27001:2022 Anhang A 8.2

Administratoren verwenden für die tägliche Arbeit ein Konto ohne erhöhte Rechte und ein getrenntes Konto für Verwaltungsaufgaben.

Prüfhandlung Prüfen, ob Administratorkonten ein Postfach besitzen oder für Internetzugriffe genutzt werden.

Nachweise Kontenliste mit Postfach, Auswertung der Internetnutzung privilegierter Konten

Schritt 05 — NIS2-Richtlinie Art. 21 Abs. 2 lit. j; § 30 Abs. 2 Nr. 10 BSIG

Für privilegierte Zugänge und für den Fernzugriff ist Mehrfaktor-Authentifizierung eingesetzt, Ausnahmen sind begründet und genehmigt.

Prüfhandlung Konfiguration von Verwaltungskonsolen, VPN und Cloud-Zugängen prüfen und die Ausnahmen durchgehen.

Nachweise Konfigurationsauszüge, Liste der Ausnahmen mit Genehmigung

Schritt 06 — ISO/IEC 27001:2022 Anhang A 8.2; BSI ORP.4

Zugangsdaten privilegierter Konten, insbesondere von Dienst- und Notfallkonten, sind in einem geschützten Tresor oder gleichwertig verwahrt und werden nach Gebrauch oder in festgelegten Abständen geändert.

Prüfhandlung Verfahren zur Verwahrung beschreiben lassen und für eine Stichprobe das Datum der letzten Änderung prüfen.

Nachweise Verfahrensbeschreibung, Auszug aus dem Tresor, Änderungsnachweise

Prüfschritte 7 bis 9

Schritt 07 — ISO/IEC 27001:2022 Anhang A 8.15 und 8.2

Administrative Tätigkeiten und die Nutzung privilegierter Konten werden protokolliert; bei besonders kritischen Systemen werden Sitzungen aufgezeichnet.

Prüfhandlung Protokollierung für zwei kritische Systeme prüfen und eine administrative Tätigkeit anhand des Protokolls nachvollziehen.

Nachweise Protokollkonfiguration, Protokollauszüge, Aufzeichnungen

Schritt 08 — ISO/IEC 27001:2022 Anhang A 5.18 und 8.2

Privilegierte Rechte werden in festgelegten Abständen durch die Verantwortlichen überprüft, Befunde werden umgesetzt.

Prüfhandlung Letzte Überprüfung ansehen: Umfang, Rücklauf, Fristen und tatsächlicher Entzug nicht mehr benötigter Rechte.

Nachweise Berichte der Überprüfung, Bestätigungen, Tickets zum Entzug

Schritt 09 — ISO/IEC 27001:2022 Anhang A 8.2

Erhöhte Rechte werden bei Bedarf zeitlich befristet vergeben und danach automatisch entzogen, wo die Technik es erlaubt.

Prüfhandlung Prüfen, ob befristete Rechte im Einsatz sind, und eine Stichprobe von Vergaben auf den Entzug nach Ablauf untersuchen.

Nachweise Konfiguration der befristeten Vergabe, Protokoll von Vergabe und Entzug

Prüfschritte 10 bis 12

Schritt 10 ISO/IEC 27001:2022 Anhang A 8.2; BSI ORP.4

Notfallzugriffe sind geregelt: Auslösung, Genehmigung, Nutzung, Protokollierung und nachträgliche Überprüfung.

Prüfhandlung Alle Nutzungen von Notfallkonten der letzten zwölf Monate ansehen und Genehmigung sowie nachträgliche Überprüfung prüfen.

Nachweise Verfahren zum Notfallzugriff, Liste der Nutzungen, Nachweise der Überprüfung

Schritt 11 ISO/IEC 27001:2022 Anhang A 5.19 und 8.2

Privilegierte Zugriffe von Dienstleistern sind vertraglich geregelt, einzeln freigegeben, befristet und protokolliert.

Prüfhandlung Zugänge von drei Dienstleistern prüfen: Freigabe, Befristung, Authentifizierung und Protokolle der letzten Sitzungen.

Nachweise Verträge, Freigaben, Zugangsprotokolle

Schritt 12 ISO/IEC 27001:2022 Anhang A 5.18; BSI ORP.4

Konten ausgeschiedener oder gewechselter Administratoren werden zeitnah gesperrt oder angepasst.

Prüfhandlung Austritts- und Wechsellisten mit den Administratorgruppen abgleichen und die Zeit bis zur Anpassung ermitteln.

Nachweise Austrittsliste, Auszug der Administratorgruppen, Sperrprotokoll

Unterlagenanforderung

Diese 8 Unterlagen vor Prüfungsbeginn anfordern

1. Richtlinie zu privilegierten Zugriffen
2. Inventar der privilegierten, technischen und Notfallkonten
3. Systemauszüge der Administratorgruppen zu einem Stichtag
4. Konfigurationsnachweise zur Mehrfaktor-Authentifizierung
5. Verfahrensbeschreibung zur Verwahrung der Zugangsdaten
6. Protokollauszüge zu administrativen Tätigkeiten
7. Berichte der letzten Überprüfung privilegierter Rechte
8. Verträge und Freigaben für Zugriffe von Dienstleistern

TYPISCHE FESTSTELLUNGEN

Es gibt keine vollständige Übersicht über privilegierte Konten; Dienstkonten haben keine verantwortliche Person.

Administratoren arbeiten täglich mit ihrem privilegierten Konto, auch für E-Mail und Internet.

Zugangsdaten von Notfall- und Dienstkonten liegen in Tabellen oder sind seit Jahren unverändert.

Mehrfaktor-Authentifizierung wird für Administratoren nicht durchgängig verlangt, Ausnahmen sind nicht begründet.

Die Überprüfung privilegierter Rechte wird bestätigt, ohne dass Rechte tatsächlich entzogen werden.

Dienstleister behalten Zugänge nach Ende des Auftrags.

Bibliothek Muster-Prüfprogramme

29 Muster-Prüfprogramme online

proauditmap.com/pruefprogramme/

Vollständiges Prüfpaket in ProAuditMap

proauditmap.com

ProAuditMap

Muster ohne Gewähr und keine Rechtsberatung. Gesetze, Verordnungen und Standards erscheinen nur als Fundstelle, Normtexte sind nicht abgedruckt. Passen Sie Umfang und Tiefe vor der Verwendung an Ihre Organisation, Ihre Risiken und die aktuelle Fassung der für Sie geltenden Vorschriften an. Stand: 13. Oktober 2026